

Мандриков Г.В., аспирант

Научный руководитель Доросинский Л.Г., проф., д-р техн. наук

ФОРМАЛЬНЫЕ МОДЕЛИ БЕЗОПАСНОСТИ

Формальные модели широко используются при построении систем защиты, так как с их помощью можно доказать безопасность системы, опираясь при этом на объективные доказуемые математические постулаты. Большое развитие получил подкласс моделей, основанных на разграничении доступа. Политика безопасности подобных систем направлена на то, чтобы информация не стала известной тому, кому не следует ее знать. Известными представителями моделей разграничения доступа являются модели, построенные по принципу предоставления прав.

Среди них можно выделить две группы:

- а) дискреционные (произвольные, избирательные);
- б) мандатные (нормативные, полномочные).

Модели дискреционного доступа (избирательное управление доступом, DAC: Discretionary Access Control).

Типы доступа, используемые в модели: read, write. Обеспечивается хорошее разделение субъектов друг от друга. Все объекты и субъекты системы должны быть идентифицированы, права доступа определяются на основе некоторого внешнего (по отношению к системе) правила (свойство избирательности). Основная идея подобных систем в том, что система защиты представляется в виде декартового произведения множеств, составными частями которых являются элементы системы защиты. Используется аппарат дискретной математики. Политика безопасности либо разрешает некоторое действие над объектом защиты, либо запрещает.

Наиболее известные: пятимерная модель Хартсона, модель Харрисона-Руззо-Ульмана, типизированная матрица доступа, монотонная типизированная матрица доступа и др.

Модели мандатного доступа (полномочное управление доступом, MAC: Mandatory Access Control).

В отличие от моделей дискреционного доступа данный тип моделей накладывает ограничение на передачу информации от одного пользователя другому. Благодаря этому в подобных системах проблемы троянских программ не существует.

Модель Белла-Лападулы, модель доверенных (уполномоченных) субъектов, модель совместного доступа, модели распределенных систем, модель LWM (Low Water Mark) являются наиболее распространенными в данной области.